এনক্রিপশন

টেক দুনিয়ায় থাকুন নিরাপদ

আপনি আর আমি এমন ভাষায় কোনো কথা বলছি যে ভাষা পৃথিবীর অন্য কেউ জানেনা!

কল্পনা করেন তো ব্যাপারটা, ইন্টারেস্টিং না?

এনক্রিপশনের ব্যাপারটা এরকম-ই। আচ্ছা Be serious!

বি.দ্র. তথ্য অপব্যবহার এর দায় কোনোক্রমেই লেখক নিবেনা।

.

[ক.]

এনক্রিপশন কী?

ইনক্রিপশন হচ্ছে এমন এক পদ্ধতি যার মাধ্যমে আপনি যখন কোন লেখা/ফাইল কাওকে পাঠানোর জন্য বা কোথাও সেভ করে রাখার জন্য বা স্টোর করার জন্য তৈরি করবেন তখন তা এমন একটি অবস্থায় বা এমন একটি ফর্মে থাকবে যাতে ডাটাটি আপনি শুধু যাকে পাঠানোর জন্য তৈরি করেছেন, যেন সেই শুধু তা অ্যাক্সেস করতে পারে। এবং ভুল করে যদি কোন অনাকাঙ্ক্ষিত ব্যাক্তির কাছে চলেও যায় তবে সে ডাটাটির কোন মতলব না বের করতে পারে। এই হচ্ছে Encryption এর মূল মন্ত্র।

.

[খ.]

এটা কিভাবে কাজ করে?

মনে করুন একটি সাধারন Encryption তৈরি করার জন্য আমি "A,B,C,D" থেকে Z পর্যন্ত A কে লিখব Z হিসেবে, B কে লিখব A হিসেবে এবং C কে লিখব B হিসেবে। এভাবেই আমি যে শব্দটি আসলে লিখতে চাচ্ছি তার আগে অক্ষর ব্যবহার করে লিখব। এখন মনে করুন আমি লিখতে চাচ্ছি ABBA, এখন উপরের নিয়ম অনুসারে Encryption করার পরে শব্দটি হবে ZAAZ। এখন কেউ যদি না জানে আমি Encryption করার জন্য একটি করে পেছনে শব্দ ব্যবহার করেছি, তবে কেউই এটা বুঝতে পারবেনা।

এখন এটা তো একটা উদাহরণ গেলো মাত্র, এর চেয়ে অনেক কঠিনও হতে পারে। ধরেন A এর বদলে লেখলাম

%, B এর বদলে লেখলাম 2, C এর বদলে C-ই লেখলাম। হেহে! বুঝেন মজা এবার!

.

[গ.]

তো এত কষ্ট করে একটা একটা করে অক্ষর লেখে সাজানোর সময় কারো আছে নাকি? তাহলে কেম্নে কি করবেন?

এর সমাধান হচ্ছে Public Key Encryption। এই পদ্ধতি একদম কমন। এবং বেশির ভাগ Encryption এর ক্ষেত্রেই এই সিস্টেম ব্যবহার করা হয়। এখন এই পাবলিক কী (Key) ইনক্রিপশনটা কি?

.

মনে করুন আমি একজন pgp ইউজার এবং আপনি pgp একজনে ইউজার। আমাদের প্রত্যেকের কাছে দুইটি করে কী (Key) থাকে। সেক্ষেত্রে আমার কাছেও দুইটি কী রয়েছে। একটি হলো প্রাইভেট কী, যেটা শুধু আমার কাছে আছে এবং আরেকটি হলো পাবলিক কী, যেটা প্রত্যেকের কাছে থাকবে। আমার পাবলিক কী আপনার কাছেও থাকবে।

.

[ঘ.]

এখন প্রশ্ন, Public বা Private Key আবার কি? দেখুন প্রাইভেট অথবা পাবলিক শব্দের অর্থ তো জানাই আছে। এখানে Key হলো মাত্র ৪-৫কেবি সাইজের একটা ফাইল। ইনক্রিপটেড ডাটা ডি-কোড করার ফর্মুলা এই Key তে থাকে। অর্থাৎ Key তে বর্ণিত থাকে যে কীভাবে একটি ইনক্রিপটেড ম্যাসেজকে অরিজিনাল ম্যাসেজে পরিনত করা যাবে।

.

এখন চলুন পাবলিক কী (Key) এবং প্রাইভেট কী (Key) সম্পর্কে কিছু গুরুত্বপূর্ণ বিষয় জেনে নেওয়া যাক।

মনে করুন আপনি কোন ম্যাসেজ বা ফাইলকে আমার পাবলিক কী ব্যবহার করে লক করে ফেললেন। তো সেই ম্যাসেজ শুধুমাত্র আমার প্রাইভেট কী দ্বারাই ওপেন করা সম্ভব। আবার যদি আমি যদি কোন ম্যাসেজকে আমার প্রাইভেট কী দ্বারা লক করি তবে সেটি শুধু মাত্র আমার পাবলিক কী (Key) ব্যবহার করেই ওপেন করা সম্ভব।

.

[ঙ.]

প্র্যাকটিকাল উদাহরণ নিন,

ধরুন কোনোভাবে AQIS এর gpg public key আপনার কাছে আছে। হতে পারে কোনো বিবৃতি বা দায় স্বীকারের মেসেজ থেকে আপনি সংগ্রহ করেছেন। আপনি একটা ফাইলে আপনার কথা রেকর্ড করে বা লেখে উনাদের পাবলিক কি দিয়ে এনক্রিপ্ট করে ফেললেন। এবার ওই এনক্রিপ্টেড ফাইলটা যেকোনো যায়গায় আপলোড করলেন। তারপর ব্লগে বা ফোরামে ফাইলটা শেয়ার তাদের দেখতে অনুরোধ করলেন। এখন ফাইলটা সবাই পেলেও ফাইলে কি আছে সেটা কেউ বুঝতে পারবেনা। একমাত্র AQIS এর প্রাইভেট কী যাদের কাছে আছে সেই কেবল ফাইলটা ডিক্রিপ্ট করতে পারবে।

অর্থাৎ আপনার বার্তা তাদের কাছে পৌঁছানোর আগে পর্যন্ত নিরাপদেই থাকবে।

.

whatsapp, telegram এর মত end-to-end encrypted মেসেঞ্জারগুলোতেও এই টেকনোলোজি ব্যাবহার করা হয়। তবে এক্ষেত্রে আমাদের key দুইটা ওদের সার্ভারে জমা থাকে, লগিন করলে যায়গামত অটোমেটিক সেট হয়ে কাজ করে।

.

[চ.]

আরেকধরণের ইজি এনক্রিপশন আছে, একটা পাসওয়ার্ড দিয়ে আপনি এনক্রিপ্ট করলেন। এরপর ওই পাসওয়ার্ড দিয়েই কেবল মেসেজ/ফাইলটা খোলা যাবে। অতিরিক্ত কি টি নাই।

.

আর ক্ষেত্র বিশেষে নিরাপত্তা বাড়াতে ২, ৩ বা এচেয়ে বেশি স্তরের এনক্রিপশনও হতে পারে।

যেমনঃ প্রথমে কোনো পাসওয়ার্ড দিয়ে এনক্রিপ্ট করলেন, এরপর প্রাপকের পাবলিক কি দিয়ে করলেন, এরপর আপনার প্রাইভেট কি দিয়ে করলেন, এরপর আবার.......

.

আবার আরেকটা এনক্রিপশন পদ্ধতি আছে, সম্ভবত এটাকে হ্যাজ টেবিল বলে। এর অনেক স্টাইল আছে, যেমনঃ MD5, SHA-1, SHA-2, BASE 64, HeX, Binary, Decimal এসবকে আমি আসলে আগে এনকোডিং বলতাম। আল্লাহই জানে আসল নাম কি।

এটার উদাহরণ এরকমঃ আমি Base64 এ hello লেখলে হবে aGVsbG8=

আপনি এবার যেকোনো Base64 Decoder দিয়ে উপরের লেখাটা ডিকোড করলেই hello লেখা পাবেন।

এবার চিন্তা করেন কোথায় aGVsbG8= আর কোথায় hello. পুলিশ যদি না জানে এটা base64 এ এনকোড করা, তাহলে যিন্দেগিতেও আপনার hello মেসেজ উদ্ধার করতে পারবেনা